前　言

本规范是根据住房和城乡建设部《2008年工程建设标准规范制订、修订计划(第二批)的通知》(建标〔2008〕105号)的要求，由中国石化工程建设有限公司会同有关单位共同编制完成的。

本规范在编制过程中，编制组经广泛调查研究，认真总结实践经验，参考有关国际标准和国外标准，并在广泛征求意见的基础上，制定本规范。

本规范共分15章。主要技术内容包括：总则，术语和缩略语，安全生命周期，安全完整性等级，设计基本原则，测量仪表，最终元件，逻辑控制器，通信接口，人机接口，应用软件，工程设计，组态、集成与调试、验收测试，操作维护、变更管理，文档管理等。

本规范由住房和城乡建设部负责管理，由中国石油化工集团公司负责日常管理，由中国石化工程建设有限公司负责具体技术内容的解释。执行过程中如有意见或建议，请寄送中国石化工程建设有限公司(地址：北京市朝阳区安慧北里安园21号，邮政编码：100101)，以供今后修订时参考。

本规范主编单位、参编单位、参加单位、主要起草人和主要审查人：

主 编 单 位： 中国石化工程建设有限公司

参 编 单 位： 中国寰球工程公司
中石化宁波工程有限公司
北京康吉森自动化设备技术有限责任公司
中石化—霍尼韦尔(天津)有限公司

参 加 单 位： 中石化洛阳工程有限公司
中石化上海工程有限公司

中国石油天然气华东勘察设计研究院
中国石油大庆石化工程有限公司
中国石化扬子石化有限公司
上海黑马安全自动化系统有限公司
北京天时盈达自动化设备有限公司

主要起草人： 黄步余　叶向东　范宗海　马　蕾　胡　晨
张建国　高生军　李　磊　林　融　胡同印
朱向暄　张悦崑　王发兵　张同科

主要审查人： 赵永登　丁兰蓉　王立奉　王成林　王胜利
刘　军　李玉明　宋志远　杨金城　林洪俊
周家祥　赵　柱　顾　铮　葛春玉　裴炳安

目　　次

Contents

1 总　　则

1.0.1 为了防止和降低石油化工工厂或装置的过程风险，保证人身和财产安全，保护环境，制定本规范。

1.0.2 本规范适用于石油化工工厂或装置新建、扩建及改建项目的安全仪表系统的工程设计。

1.0.3 石油化工安全仪表系统的工程设计，除应符合本规范外，尚应符合国家现行有关标准的规定。

2 术语和缩略语

2.1 术　　语

2.1.1 安全仪表系统　　safety instrumented system

实现一个或多个安全仪表功能的仪表系统。

2.1.2 风险　　risk

预期可能发生的特定危险事件和后果。

2.1.3 过程风险　　process risk

因非正常事件引起过程条件改变而产生的风险。

2.1.4 安全生命周期　　safety life cycle

从工程方案设计开始到所有安全仪表功能停止使用的全部时间。

2.1.5 危险　　hazard

导致人身伤害或疾病、财产损失、环境破坏等事件的可能。

2.1.6 风险评估　　risk assessment

评估风险大小以及确定风险容许程度的全过程。

2.1.7 保护层　　protection layer

通过控制、预防、减缓等手段降低风险的措施。

2.1.8 安全功能　　safety function

为了达到或保持过程的安全状态，由安全仪表系统、其他安全相关系统或外部风险降低设施实现的功能。

2.1.9 安全仪表功能　　safety instrumented function

为了防止、减少危险事件发生或保持过程安全状态，用测量仪表、逻辑控制器、最终元件及相关软件等实现的安全保护功能或安全控制功能。

2.1.10 故障　　fault

可导致功能单元执行能力降低或丧失的异常状况。

2.1.11 安全完整性　　safety integrity

在规定的条件和时间内，安全仪表系统完成安全仪表功能的平均概率。

2.1.12 安全完整性等级　　safety integrity level

安全功能的等级。安全完整性等级由低到高为 SIL1～ SIL4。

2.1.13 失效　　failure

功能单元某种功能或执行能力的终止。

2.1.14 危险失效　　dangerous failure

可导致安全仪表系统处于潜在危险或丧失功能的失效。

2.1.15 安全失效　　safe failure

不可能导致安全仪表系统处于潜在危险或丧失功能的失效。

2.1.16 测量仪表　　sensor

安全仪表系统的组成部分，用于测量过程变量的设备。

2.1.17 逻辑控制器　　logic solver

安全仪表系统的组成部分，执行逻辑功能的设备。

2.1.18 最终元件　　final element

安全仪表系统的组成部分，执行逻辑控制器指令或设定的动作，使过程达到安全状态的设备。

2.1.19 基本过程控制系统　　basic process control system

响应过程测量以及其他相关设备、其他仪表、控制系统或操作员的输入信号，按过程控制规律、算法、方式，产生输出信号实现过程控制及其相关设备运行的系统。

2.1.20 故障安全　　fail safe

安全仪表系统发生故障时，使被控制过程转入预定安全状态。

2.1.21 冗余　　redundancy

采用独立执行同一个功能的两个或多个部件或系统，互为备用及切换。

2.1.22 容错　　fault tolerant

在出现故障或错误时，功能单元仍继续执行规定功能的能力。

2.1.23 开关量 digital variable

只有0或1两个数值的变量，用来表示事物或事件的状态。也称为数字变量。

2.1.24 开关 switch

具有两种稳定位置的状态器件。有软件开关和硬件开关。

2.1.25 按钮 push button

只有一种稳定位置的状态器件。有软件按钮和硬件按钮。

2.1.26 触点 mechanical contact

由导电的金属元件组成的机械式电气器件。在外界因素作用下可以改变接通或断开导电状态。

2.1.27 接点 contact

在外界因素作用下可以改变接通或断开导电状态的电气器件。有机械式和电子式。在可编程序逻辑控制器的运算部件中还有软件接点。

2.1.28 常闭接点 normally closed contact

在没有外界因素影响时，自然情况下闭合的接点。

2.1.29 常开接点 normally open contact

在没有外界因素影响时，自然情况下断开的接点。

2.1.30 可编程电子系统 programmable electronic system

基于可以按功能需要编制或改变运行程序的电子设备，用于控制、保护或监视的系统。

2.2 缩 略 语

BPCS(Basic Process Control System)	基本过程控制系统
CPU(Central Process Unit)	中央处理单元
EMC(Electro-Magnetic Compatibility)	电磁兼容性
FAT(Factory Acceptance Testing)	工厂验收测试
FLD(Functional Logic Diagram)	功能逻辑图
FBD(Functional Block Diagram)	功能块图

FDS(Functional Design Specification)	功能设计规定
HAZOP(Hazard and Operability Study)	危险和可操作性研究
HMI(Human Machine Interface)	人机接口
HSE(Health,Safety and Environment)	健康、安全和环保
MOS(Maintenance Override Switch)	维护旁路开关
OOS(Operational Override Switch)	操作旁路开关
PES(Programmable Electronic System)	可编程电子系统
PHA(Preliminary Hazard Analysis)	预危险分析
PFD_{avg}(Probability of Failure on Demand Average)	低要求模式的平均失效概率
PLC(Programmable Logic Controller)	可编程逻辑控制器
SAT(Site Acceptance Testing)	现场验收测试
SER(Sequence Event Recorder)	事件顺序记录
SIF(Safety Instrumented Function)	安全仪表功能
SIL(Safety Integrity Level)	安全完整性等级
SIS(Safety Instrumented System)	安全仪表系统
UPS(Uninterruptable Power Supply)	不间断电源

3 安全生命周期

3.1 一 般 规 定

3.1.1 石油化工工厂或装置工程设计中，应确定安全仪表系统的安全生命周期内各阶段工作所需要的管理活动。

3.1.2 安全生命周期宜分为工程设计阶段、集成调试及验收测试阶段和操作维护阶段。

3.1.3 安全生命周期工作(图 3.1.3)宜包括工程方案设计，过程

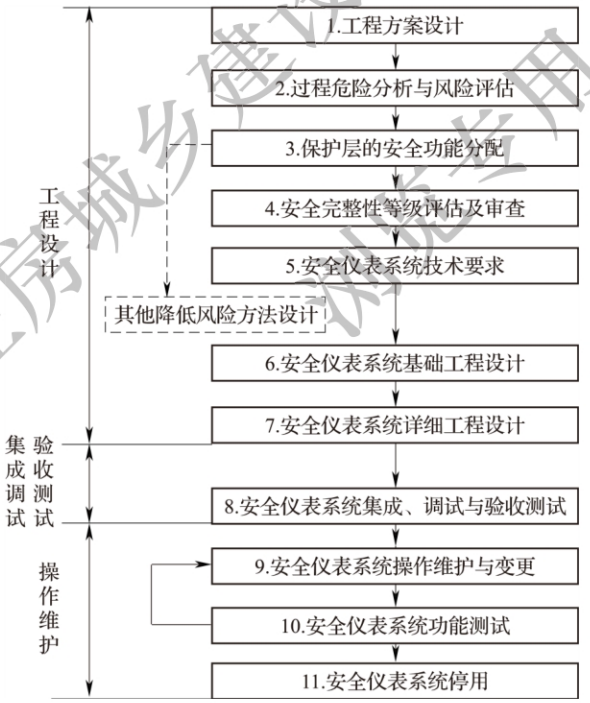

图 3.1.3 安全生命周期工作流程

危险分析与风险评估，保护层的安全功能分配，安全完整性等级评估及审查，安全仪表系统技术要求，安全仪表系统基础工程设计，安全仪表系统详细工程设计，安全仪表系统集成、调试及验收测试，安全仪表系统操作维护与变更，安全仪表系统功能测试，安全仪表系统停用等。

3.2 工 程 设 计

3.2.1 工程方案设计宜包括初步的过程危险分析、主要安全控制策略和措施及相应的说明。

3.2.2 过程危险分析和风险评估宜包括识别过程及相关设备的危险事件及原因，危险事件发生的顺序、可能性及后果，确定降低风险的要求和措施，确定安全仪表功能等。过程危险分析和风险评估宜采用危险和可操作性研究方法或预危险分析方法，也可采用安全检查表、故障模式和影响分析、因果分析方法等。

3.2.3 保护层安全功能的分配可包括分配预防、控制或减缓过程危险的保护层安全功能，分配安全仪表功能的风险降低目标。保护层的安全功能分配应符合现行国家标准《电气/电子/可编程电子安全相关系统的功能安全》GB/T 20438 和《过程工业领域安全仪表系统的功能安全》GB/T 21109 的有关规定。

3.2.4 安全完整性等级可根据过程危险分析和保护层功能分配的结果评估并确定。

3.2.5 安全仪表系统技术要求可包括安全仪表功能及安全完整性等级、过程安全状态、操作模式、检验测试间隔时间等。

3.2.6 安全仪表系统的基础工程设计宜包括安全仪表系统设计说明、安全仪表系统规格书、安全联锁因果表或功能说明等。

3.2.7 安全仪表系统的详细工程设计宜包括安全仪表系统设计说明、安全仪表系统规格书、功能逻辑图、组态编程等。

3.3 集成、调试及验收测试

3.3.1 安全仪表系统集成、调试及验收测试，应符合安全仪表系统规格书及功能逻辑图的技术要求。

3.3.2 安全仪表系统调试结果应符合安全仪表系统技术要求。

3.3.3 安全仪表系统验收测试应包括工厂验收和现场验收。安全仪表系统硬件、系统软件和应用软件等，应符合安全仪表系统技术要求。

3.4 操 作 维 护

3.4.1 操作维护应遵循操作维护作业程序，应使操作维护过程符合安全仪表系统技术要求的功能安全。

3.4.2 安全仪表系统的硬件和应用软件的修改或变更应符合变更修改程序，并应按审批程序获得授权批准，不应改变设计的安全完整性等级，并应保留变更记录。

3.4.3 操作维护人员应定期培训，培训内容宜包括安全仪表系统的功能、可预防的过程危险、测量仪表和最终元件、安全仪表系统的逻辑动作、安全仪表系统及过程变量的报警、安全仪表系统动作后的处理等。

3.4.4 功能测试间隔应按安全仪表系统的技术要求确定，并应按测试程序进行功能测试。

3.4.5 安全仪表系统的停用应进行审查并得到批准。安全仪表系统更新应制订更新程序。更新后的安全仪表系统应能实现规定的安全仪表功能。

4 安全完整性等级

4.1 一 般 规 定

4.1.1 安全完整性宜包括硬件安全完整性和系统安全完整性。

4.1.2 安全完整性等级可分为 SIL 1、SIL 2、SIL 3、SIL 4。

4.1.3 在低要求操作模式时，安全仪表功能的安全完整性等级应采用平均失效概率衡量，宜根据表 4.1.3 确定。

表 4.1.3 安全仪表功能的安全完整性等级(低要求操作模式)

安全完整性等级(SIL)	低要求操作模式的平均失效概率(PFD_{avg})
4	$\geqslant 10^{-5}$且$<10^{-4}$
3	$\geqslant 10^{-4}$且$<10^{-3}$
2	$\geqslant 10^{-3}$且$<10^{-2}$
1	$\geqslant 10^{-2}$且$<10^{-1}$

4.1.4 在高要求操作模式时，安全仪表功能的安全完整性等级应采用每小时危险失效频率衡量，宜根据表 4.1.4 确定。

表 4.1.4 安全仪表功能的安全完整性等级(高要求操作模式)

安全完整性等级(SIL)	高要求操作模式的危险失效频率(每小时)
4	$\geqslant 10^{-9}$且$< 10^{-8}$
3	$\geqslant 10^{-8}$且$< 10^{-7}$
2	$\geqslant 10^{-7}$且$< 10^{-6}$
1	$\geqslant 10^{-6}$且$< 10^{-5}$

4.2 安全完整性等级评估

4.2.1 安全完整性等级评估宜包括下列内容：

1 确定每个安全仪表功能的安全完整性等级；

2　确定诊断、维护和测试要求等。

4.2.2　安全完整性等级评估方法应根据工艺过程复杂程度、国家现行标准、风险特性和降低风险的方法、人员经验等确定。主要方法应包括保护层分析法、风险矩阵法、校正的风险图法、经验法及其他方法。

4.2.3　安全完整性等级评估宜采用审查会方式。审查的主要文件宜包括工艺管道与仪表流程图、工艺说明书、装置及设备布置图、危险区域划分图、安全联锁因果表及其他有关文件。参加评估的主要人员宜包括工艺、过程控制(仪表)、安全、设备、生产操作及管理等方面。

5 设计基本原则

5.0.1 安全仪表系统的工程设计应满足石油化工工厂或装置的安全仪表功能、安全完整性等级等要求。

5.0.2 安全仪表系统的工程设计应兼顾可靠性、可用性、可维护性、可追溯性和经济性，应防止设计不足或过度设计。

5.0.3 安全仪表系统应由测量仪表、逻辑控制器和最终元件等组成。

5.0.4 安全仪表系统的功能应根据过程危险及可操作性分析，人员、过程、设备及环境的安全保护，以及安全完整性等级等要求确定。

5.0.5 石油化工工厂或装置的安全完整性等级不应高于SIL 3级。

5.0.6 安全仪表系统应符合安全完整性等级要求。安全完整性等级可采用计算安全仪表系统的失效概率的方法确定。

5.0.7 安全仪表系统可实现一个或多个安全仪表功能，多个安全仪表功能可使用同一个安全仪表系统。当多个安全仪表功能在同一个安全仪表系统内实现时，系统内的共用部分应符合各功能中最高安全完整性等级要求。

5.0.8 安全仪表系统应独立于基本过程控制系统，并应独立完成安全仪表功能。

5.0.9 安全仪表系统不应介入或取代基本过程控制系统的工作。

5.0.10 基本过程控制系统不应介入安全仪表系统的运行或逻辑运算。

5.0.11 安全仪表系统应设计成故障安全型。当安全仪表系统内部产生故障时，安全仪表系统应能按设计预定方式，将过程转入安全状态。

5.0.12 安全仪表系统的逻辑控制器应具有硬件和软件自诊断功能。

5.0.13 安全仪表系统的中间环节应少。

5.0.14 逻辑控制器的中央处理单元、输入输出单元、通信单元及电源单元等，应采用冗余技术。

5.0.15 安全仪表系统应根据国家现行有关防雷标准的规定实施系统防雷工程。

5.0.16 安全仪表系统的交流供电宜采用双路不间断电源的供电方式。

5.0.17 安全仪表系统的接地应采用等电位连接方式。

5.0.18 安全仪表系统的硬件、操作系统及编程软件应采用正式发布版本。

5.0.19 安全仪表系统软件、编程、升级或修改等文档应备份。

5.0.20 安全仪表系统内的设备宜设置同一时钟。

5.0.21 在大型石油化工项目中设置多套安全仪表系统时，每套系统应能独立工作。

5.0.22 当安全仪表系统输入、输出信号线路中有可能存在来自外部的危险干扰信号时，应采取隔离器、继电器等隔离措施。

6 测 量 仪 表

6.1 一 般 规 定

6.1.1 测量仪表包括模拟量和开关量测量仪表，安全仪表系统宜采用模拟量测量仪表。

6.1.2 测量仪表宜采用 4mA～20mA 叠加 HART 传输信号的智能变送器。

6.1.3 在爆炸危险场所，测量仪表应采用隔爆型或本安型。当采用本安系统时，应采用隔离式安全栅。

6.1.4 现场安装的测量仪表，防护等级不应低于 IP 65。

6.1.5 测量仪表不应采用现场总线或其他通信方式作为安全仪表系统的输入信号。

6.1.6 测量仪表及取源点宜独立设置。

6.1.7 测量仪表的性能和设置应满足安全完整性等级要求。

6.2 测量仪表的独立设置

6.2.1 SIL 1 级安全仪表功能，测量仪表可与基本过程控制系统共用。

6.2.2 SIL 2 级安全仪表功能，测量仪表宜与基本过程控制系统分开。

6.2.3 SIL 3 级安全仪表功能，测量仪表应与基本过程控制系统分开。

6.3 测量仪表的冗余设置

6.3.1 SIL 1 级安全仪表功能，可采用单一测量仪表。

6.3.2 SIL 2 级安全仪表功能，宜采用冗余测量仪表。

6.3.3 SIL 3 级安全仪表功能，应采用冗余测量仪表。

6.4 测量仪表的冗余方式

6.4.1 当系统要求高安全性时，应采用“或”逻辑结构。

6.4.2 当系统要求高可用性时，应采用“与”逻辑结构。

6.4.3 当系统需要兼顾高安全性和高可用性时，宜采用三取二逻辑结构。

6.5 开关量测量仪表

6.5.1 开关量测量仪表可包括过程变量开关、手动开关、按钮、继电器触点等。

6.5.2 紧急停车用的开关量测量仪表，正常工况时，触点应处于闭合状态；非正常工况时，触点应处于断开状态。

6.5.3 重要的输入回路宜设置线路开路和短路故障检测。输入回路的开路和短路故障，宜在安全仪表系统中报警和记录。

7 最终元件

7.1 一般规定

7.1.1 最终元件应包括控制阀(调节阀、切断阀)、电磁阀、电机等。

7.1.2 最终元件宜采用气动控制阀,不宜采用电动控制阀。

7.1.3 最终元件的设置应满足安全完整性等级要求。

7.2 控制阀的独立设置

7.2.1 SIL 1 级安全仪表功能,控制阀可与基本过程控制系统共用,应确保安全仪表系统的动作优先。

7.2.2 SIL 2 级安全仪表功能,控制阀宜与基本过程控制系统分开。

7.2.3 SIL 3 级安全仪表功能,控制阀应与基本过程控制系统分开。

7.3 控制阀的冗余设置

7.3.1 SIL 1 级安全仪表功能,可采用单一控制阀。

7.3.2 SIL 2 级安全仪表功能,宜采用冗余控制阀。

7.3.3 SIL 3 级安全仪表功能,应采用冗余控制阀。

7.3.4 控制阀冗余方式可采用一个调节阀和一个切断阀,也可采用两个切断阀。

7.4 控制阀附件的配置

7.4.1 调节阀带的电磁阀应安装在阀门定位器与执行器之间。切断阀带的电磁阀应安装在执行器上。

7.4.2 在爆炸危险场所，电磁阀和阀位开关应采用隔爆型或本安型。当采用本安型时，应采用隔离式安全栅。

7.4.3 现场安装的电磁阀和阀位开关，防护等级不应低于IP 65。

7.4.4 电磁阀宜采用24VDC长期励磁型，电磁阀电源应由安全仪表系统提供。

7.4.5 当系统要求高安全性时，冗余电磁阀宜采用“或”逻辑结构；当系统要求高可用性时，冗余电磁阀宜采用“与”逻辑结构。

8 逻辑控制器

8.1 一般规定

8.1.1 逻辑控制器宜采用可编程电子系统。对于输入、输出点数较少、逻辑功能简单的场合，逻辑控制器可采用继电器系统。逻辑控制器也可采用可编程电子系统和继电器系统混合构成。

8.1.2 用于逻辑控制器的可编程电子系统应取得国家权威机构的功能安全认证。

8.1.3 逻辑控制器的响应时间应包括输入、输出扫描处理时间与中央处理单元运算时间，宜为100ms～300ms。

8.1.4 逻辑控制器的中央处理单元负荷不应超过50%。

8.1.5 逻辑控制器的内部通信负荷不应超过50%，采用以太网的通信负荷不应超过20%。

8.2 逻辑控制器的独立设置

8.2.1 SIL 1级安全仪表功能，逻辑控制器宜与基本过程控制系统分开。

8.2.2 SIL 2级安全仪表功能，逻辑控制器应与基本过程控制系统分开。

8.2.3 SIL 3级安全仪表功能，逻辑控制器应与基本过程控制系统分开。

8.3 逻辑控制器的冗余设置

8.3.1 SIL 1级安全仪表功能，可采用冗余逻辑控制器。

8.3.2 SIL 2级安全仪表功能，宜采用冗余逻辑控制器。

8.3.3 SIL 3 级安全仪表功能，应采用冗余逻辑控制器。

8.4 逻辑控制器的配置

8.4.1 逻辑控制器应符合安全完整性等级要求，应独立完成安全仪表功能。

8.4.2 逻辑控制器硬件和软件版本应是正式发布版本。

8.4.3 逻辑控制器宜与基本过程控制系统的时钟保持一致。

8.4.4 逻辑控制器所有部件应满足安装环境的防电磁干扰、防腐蚀、防潮湿、防锈蚀等要求。

8.4.5 逻辑控制器的中央处理单元、输入单元、输出单元、电源单元、通信单元等应为独立的单元，应允许在线更换单元而不影响逻辑控制器的正常运行。

8.4.6 逻辑控制器应有硬件和软件的诊断和测试功能。诊断和测试信息应在工程师站或操作站显示、记录。

8.4.7 逻辑控制器的系统故障宜在安全仪表系统的操作站报警，也可在基本过程控制系统的操作站报警。

8.5 逻辑控制器的接口配置

8.5.1 输入、输出卡件信号通道应带光电或电磁隔离。

8.5.2 检测同一过程变量的多台变送器信号宜接到不同输入卡件。

8.5.3 冗余的最终元件应接到不同的输出卡件，每一输出信号通道应只接一个最终元件。

8.5.4 输入、输出卡件不应采用现场总线数字信号。

8.5.5 本安回路应采用隔离型安全栅。

8.5.6 需要线路检测的回路，应采用带有线路短路和开路检测功能的输入、输出卡。

9 通 信 接 口

9.1 一 般 规 定

9.1.1 安全仪表系统与基本过程控制系统通信宜采用RS 485串行通信接口，MODBUS RTU或TCP/IP通信协议。

9.1.2 安全仪表系统与基本过程控制系统通信接口宜冗余配置。冗余通信接口应有诊断功能。

9.1.3 安全仪表系统与基本过程控制系统通信不应通过工厂管理网络传输。

9.1.4 除旁路信号和复位信号外，基本过程控制系统不应采用通信方式向安全仪表系统发送指令。

9.1.5 除基本过程控制系统外，安全仪表系统与其他系统之间不应设置通信接口。安全仪表系统与其他系统之间的连接应采用硬接线方式。

9.2 通信接口的配置

9.2.1 通信接口的故障不应影响安全仪表系统的安全功能。通信接口故障应在操作站或工程师站显示、报警。

9.2.2 网络通信接口负荷不应超过50%。

10 人机接口

10.1 操作员站

10.1.1 安全仪表系统宜设操作员站。在操作员站失效时，安全仪表系统的逻辑处理功能不应受影响。

10.1.2 安全仪表系统应采用操作员站作为过程信号报警和联锁动作报警的显示和记录。

10.1.3 操作员站不应修改安全仪表系统的应用软件。

10.1.4 操作员站设置的软件旁路开关应加键锁或口令保护，并应设置旁路状态报警和记录。

10.1.5 操作员站应提供程序运行，联锁动作，输入、输出状态，诊断结果等显示，并应具有报警及记录等功能。

10.2 辅助操作台

10.2.1 紧急停车按钮、开关、信号报警器及信号灯等，应安装在安全仪表系统的辅助操作台。

10.2.2 信号报警可采用信号报警器显示。

10.2.3 信号报警器应采用下列颜色的灯光：

1 红色灯光表示越限报警或紧急状态；

2 黄色灯光表示预报警；

3 绿色灯光表示运转设备或过程变量正常。

10.2.4 关键信号报警除在操作员站显示外，应同时在辅助操作台显示。

10.2.5 紧急停车按钮、开关、信号报警器等与安全仪表系统连接，应采用硬接线方式，不应采用通信方式。紧急停车按钮应采用红色，旁路开关宜采用黄色，确认按钮宜采用黑色，试验按钮宜采

用白色。

10.2.6 紧急停车按钮、开关、信号报警器等与安全仪表系统相距较远的场合，应采用远程输入、输出接口或远程控制器方式进行信号连接。

10.3 维护旁路开关的设置

10.3.1 维护旁路开关可按下列方式设置：

1 在安全仪表系统的操作员站设置软件开关；

2 在基本过程控制系统的操作员站设置软件开关；

3 在辅助操作台或机柜设置硬件开关。

10.3.2 采用软件开关的方式时，每个安全联锁单元宜设硬件旁路开关作为软件开关的“允许”条件。

10.3.3 维护旁路开关应设置在输入信号通道上；维护旁路开关的动作应设置报警和记录。

10.4 操作旁路开关的设置

10.4.1 操作旁路开关可按下列方式设置：

1 在安全仪表系统的操作员站设置软件开关；

2 在基本过程控制系统的操作员站设置软件开关；

3 在辅助操作台设置硬件开关。

10.4.2 当工艺过程变量从初始值变化到工艺条件正常值，信号状态不改变时，不应设置操作旁路开关；当工艺过程变量从初始值变化到工艺条件正常值，信号状态发生改变时，应设置操作旁路开关。

10.4.3 操作旁路开关应设置在输入信号通道上；操作旁路开关的动作应设置报警和记录。

10.5 复位按钮的设置

10.5.1 复位按钮可按下列方式设置：

1 在安全仪表系统的操作员站设置软件按钮；

2 在基本过程控制系统的操作员站设置软件按钮；

3 在辅助操作台设置硬件按钮。

10.5.2 复位按钮的动作应设置报警和记录。

10.6 紧急停车按钮的设置

10.6.1 紧急停车按钮应设置在辅助操作台上。

10.6.2 紧急停车按钮动作应设状态报警和记录。

10.6.3 紧急停车按钮不应设维护旁路开关或操作旁路开关。

10.7 工程师站及事件顺序记录站

10.7.1 安全仪表系统应设工程师站。工程师站应用于安全仪表系统组态编程、系统诊断、状态监测、编辑、修改及系统维护。

10.7.2 工程师站应设不同级别的权限密码保护。工程师站应显示安全仪表系统动作和诊断状态。

10.7.3 安全仪表系统应设事件顺序记录站。事件顺序记录站可单独设置，也可与安全仪表系统的工程师站共用。

10.7.4 事件顺序记录站应记录每个事件的时间、日期、标识、状态等。事件顺序记录站应设密码保护。

10.7.5 工程师站和事件顺序记录站，宜采取防病毒等保护措施。

10.7.6 工程师站和事件顺序记录站应采用台式计算机。

11 应用软件

11.1 组态及编程

11.1.1 应用软件的逻辑功能应采用布尔逻辑及布尔代数运算规则。应用软件的逻辑设计宜采用正逻辑。

11.1.2 应用软件的组态宜采用功能逻辑图或布尔逻辑表达式。

11.1.3 应用软件的组态应使用制造厂的标准组态工具软件。

11.1.4 应用软件组态工具软件应具有下列功能：

1 区分应用软件版本；

2 组态检查；

3 提供标准功能模块；

4 组态管理、仿真及测试。

11.2 应用软件的安全性

11.2.1 应用软件的安全控制应包括应用软件设计、软件组态及编程、软件集成、软件运行和维护管理、系统确认等。

11.2.2 应用软件组态编程应进行离线测试后再下载投入运行。

11.2.3 数据宜采用光盘进行复制，磁介质文件的复制应防止病毒。

11.2.4 应用软件应同时进行本地备份和异地备份。

11.3 应用软件设计和组态

11.3.1 应用软件文件应包括下列内容：

1 应用软件说明；

2 输入点、输出点、通信点清单；

3 功能逻辑图；

4　文档要求。

11.3.2　逻辑设计应具有可读性，复杂功能逻辑图应有相应的逻辑功能说明。

11.3.3　应用软件组态编程应与功能逻辑图、因果表或逻辑功能说明一致。程序执行顺序及时间应符合过程安全的要求。

11.3.4　应用软件组态文件应包括功能逻辑图、用户手册、使用说明等。

11.3.5　采用逻辑语言的软件组态文件还应包括源程序、程序说明等。

12 工 程 设 计

12.1 基础工程设计

12.1.1 安全仪表系统测量仪表、安全仪表控制系统、安全仪表系统最终元件的技术规格书，应根据安全完整性等级进行编制。

12.1.2 安全仪表系统基础工程设计文件应根据工艺安全联锁说明、工艺管道及仪表流程图等进行编制，应包括下列内容：

1 功能逻辑图、因果表及复杂逻辑功能说明；

2 安全仪表控制系统技术规格书；

3 安全仪表系统测量仪表、安全仪表系统最终元件的选型原则及技术规格书。

12.1.3 安全仪表控制系统技术规格书应包括下列主要内容：

1 基本要求；

2 选型原则；

3 控制器；

4 操作员站；

5 辅助操作台；

6 工程师站和事件顺序记录站；

7 应用软件组态；

8 系统通信；

9 系统负荷；

10 维护和安全、可靠性；

11 系统供电及接地；

12 验收测试要求；

13 环境要求；

14 机械要求；

15　技术服务；

16　质量保证；

17　文档资料。

12.1.4　安全仪表系统测量仪表、安全仪表系统最终元件的技术规格书应包括项目应用环境和条件、设计条件和约束条件、技术说明和规定、技术数据表等。

12.2　详细工程设计

12.2.1　安全仪表系统详细工程设计文件应根据安全仪表系统基础工程设计文件及详细工程设计阶段的要求进行编制，应包括下列内容：

1　安全仪表控制系统技术规格书；

2　硬件配置图；

3　功能逻辑图、因果表及复杂逻辑功能说明；

4　输入、输出点清单；

5　联锁及报警设定值；

6　应用软件需要的技术资料。

12.2.2　安全仪表控制系统合同技术附件，应包括系统硬件清单，软件清单，应用软件组态、生成、调试、操作和维护培训，工厂验收，现场验收及现场服务等。

12.2.3　详细工程设计文件应包括下列内容：

1　系统总说明及配置图；

2　操作站及机柜布置图；

3　输入、输出卡件及端子布置图、接线图；

4　供电及接地系统图；

5　远程控制器或远程输入、输出卡件及端子布置、接线图；

6　回路接线图；

7　电缆（光缆）连接表；

8　其他。

13 组态、集成与调试、验收测试

13.1 组态、集成与调试

13.1.1 安全仪表控制系统工程文件应包括下列主要内容：

1 系统硬件规格书；

2 系统软件规格书；

3 系统配置图；

4 机柜布置及接线图；

5 系统供电图；

6 系统接地图；

7 负荷计算表；

8 功耗计算表；

9 输入卡、输出卡点分配表；

10 组态编程文件(源程序、功能逻辑图等)；

11 操作维护手册。

13.1.2 工程师站、操作员站、事件顺序记录站、辅助操作台、系统柜、端子柜、安全栅柜、继电器柜、电源柜、网络柜等集成，应符合详细工程设计的规定。

13.1.3 应用软件组态应满足功能逻辑图和因果表的要求。系统软件、应用软件编译、调试及下装，应经过完整、详细地检查和测试。

13.2 验 收 测 试

13.2.1 验收测试应包括工厂验收测试、工厂联合测试和现场验收测试。

13.2.2 工厂验收测试应包括下列主要内容：

1　制造厂提供验收测试程序、测试内容及步骤；

2　验收测试报告文件、测试用的标准仪器检查；

3　全部工程文件检查；

4　硬件测试及检查；

5　系统冗余和容错功能检验；

6　系统在线可维护性测试，包括在线更换卡件、在线修改及下装软件；

7　应用程序的逻辑功能测试；

8　验收测试完成，测试报告签字。

13.2.3　工厂联合测试应包括下列主要内容：

1　与基本过程控制系统的工厂联合测试宜在基本过程控制系统制造厂进行；

2　在基本过程控制系统工厂完成安全仪表系统通信测试、软件画面测试等；

3　与其他控制系统的工厂联合测试宜在安全仪表系统制造厂进行；

4　在安全仪表系统制造厂完成与其他控制系统的通信测试、软件画面测试等；

5　工厂联合测试完成，测试报告签字。

13.2.4　现场验收测试应包括下列主要内容：

1　编制现场验收测试程序、测试内容及步骤；

2　检查工程设计文件及有关资料；

3　系统安装、系统各类连接及通电条件检查；

4　检查各项冗余功能及在线更换卡件功能；

5　操作站显示画面联合测试；

6　辅助操作台紧急停车及报警功能检查；

7　系统网络功能测试；

8　系统诊断功能测试；

9　现场验收测试完成，测试报告签字。

14 操作维护、变更管理

14.0.1 操作维护管理应包括操作维护规程、维护人员职责、定期诊断测试计划及报告、停车期间的系统检查、维护旁路开关及操作旁路开关的使用等。

14.0.2 变更管理应包括变更原因及方案、系统的版本升级、增减或修改逻辑、审核评估变更方案、确认变更的安全仪表功能、变更方案的设计与实施、变更软件功能的离线测试与检查、变更报告及操作维护规程更新等。

15 文档管理

15.0.1 安全生命周期各阶段的文档应包括安全仪表系统的工程设计、应用软件组态编程、设计审查等文件，磁介质和纸介质文件应同时存档保存。

15.0.2 文档管理应包括文件命名规则、文件格式、文件传递方式、文件控制规程、文件审核流程及文件版本管理等。

本规范用词说明

1 为便于在执行本规范条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的：

正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况下均应这样做的：

正面词采用“应”，反面词采用“不应”或“不得”；

3）表示允许稍有选择，在条件许可时首先应这样做的：

正面词采用“宜”，反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的，采用“可”。

2 条文中指明应按其他有关标准执行的写法为：“应符合……的规定”或“应按……执行”。

引用标准名录

《电气/电子/可编程电子安全相关系统的功能安全》GB/T 20438
《过程工业领域安全仪表系统的功能安全》GB/T 21109